## REMARKS

Claims 1-15 are pending in the instant application (hereinafter, the "'320 Application"). Claims 5 and 7 are amended to tie the recited method(s) to a computer system. Claim 14 is newly added to clarify capabilities of the prover and verifier agents of claim 5. The amendments to claims 5, 7 and 14 are supported throughout the '320 Application as filed, including paragraphs [0007], [0022]-[0024] and [0029]-[0033].

Claim 6 is amended for clarity, pursuant support from at least paragraph [0013] of the specification.

Claim 15 is newly added, and is equivalent to claim 7 rewritten in independent form. Per the Examiner's indication of allowable subject matter (see page 9 of the instant office action), claim 15 is believed allowable.

It is believed that the above amendments and the following remarks address and resolve each rejection presented in the Office Action mailed 08 October 2008.

### Response to Amendment

Applicants thank the Examiner for his thorough explanation of the rejections presented in the previous Office Action (mailed 08 October 2008). The Examiner's comments are addressed in responding to the pending claim rejections, below.

### Claim Rejections – 35 U.S.C. § 101

Claims 5-7 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. In particular, the Examiner states that the preamble "The method including steps of… is broad enough that the claim could be completely performed mentally, verbally or without a machine, nor is any transformation apparent." Office Action, item 12, pages 4-5. Given the amendment to claim 5, Applicant respectfully disagrees.

Claim 5 is amended to recite a method of protecting a host computer from unauthorized access by a client computer over a computer network. Claim 5 now specifies that prover and verifier agents are installed on client and host computers, respectively; that a trusted source application is created on the computer network, and that dialog between the prover and verifier occurs over a computer network. The

amendments to claim 5 make clear that the claimed method is performed by a computer system including at least two computers (host and client), and not mentally, verbally or without a machine. The amendments to claim 5 are fully supported by the specification, for example at paragraphs [0007] and [0029]-[0033]; see also FIG. 5.

Claims 6 and 7 depend from claim 5 and benefit from like argument. Claim 7 is also amended as necessary to reflect the amendments to claim 5 and to place first and second agents in additional computers on the network of claim 5. See, e.g., paragraphs [0022]-[0024] for exemplary support for the amendments to claim 7.

Applicant respectfully requests reconsideration of claims 5-7, and withdrawal of the rejection under 35 U.S.C. §101.

**Claim Rejections – 35 U.S.C. § 102 - Vallee**

Claims 5 and 6 stand rejected under 35 U.S.C. §102(e) as being anticipated by Vallee. Applicants respectfully disagree. In order to anticipate claims 5 and 6, Vallee must teach every element of each claim and "the ***identical invention*** must be shown in as complete detail as contained in the ... claim." *MPEP 2131*, citing *Verdegaal Bros. V. Union Oil Co. of California*, 814 F.2d 628, 2 USPQ2d 1051 (Fed. Cir. 1987) and *Richardson v. Suzuki Motor Co.*, 868 F2.d 1226, 9 USPQ2d 1913 (Fed. Cir. 1989), emphasis added.

*Independent Claim 5*: Thus, in order to anticipate claim 5 (as amended), Vallee must teach a method of protecting a host computer from unauthorized access by a client computer over a computer network, including the following steps:

**(a)** installing a prover agent application on the client computer;

**(b)** installing a verifier agent application on the host computer;

**(c)** creating a trusted source application on the computer network to generate and publish encrypted values of a secret and product of first and second large prime numbers;

**(d)** reading the encrypted values for the secret and product, by the prover and verifier **from the trusted source**;

**(e)** decrypting the secret, by the prover and verifier;

**(f)** decrypting the product, by the prover and verifier; and

**(g)** performing a plurality of verification dialog between the prover and verifier over the network, wherein the prover demonstrates knowledge of the secret and product without exposing the values of the secret and product, and wherein the client is denied access to a secure area of the host when the prover fails to demonstrate knowledge of the secret and product and granted access to the secure area when the client succeeds in demonstrating knowledge of the secret and product.

However, Vallee does not teach each of the above steps, nor does Vallee show the steps in as complete detail as shown in the claim.

Claim 5 recites generation and publication (by a trusted source application) of encrypted values of a *secret* and a product of first and second large *prime* numbers. See step **(c)**, above. The Examiner cites Vallee paragraphs 96-97 as anticipating this feature. However, this section recites that entity A to be authenticated chooses a random integer r, and computes an engagement $x = r^2 \text{mod} n$, which is sent to authenticator entity B.

First, entity A is an entity to be authenticated, and not a "trusted source," as recited in claim 5.

Second, none of the values in the computed engagement – x, r or n – are Vallee's secret, nor is the secret used to generate these values. Vallee specifies a "secret key $K_S$ [that] includes an integer number called the secret exponent s." Vallee paragraph [0049].

Furthermore, Vallee does not specify, at paragraphs [0096]-[0097] or elsewhere, generating a product of two large prime numbers. Thus, there is also no generation/publication of an encrypted value of a product of first and second large primes. Vallee does not anywhere discuss multiplying two large prime numbers. At paragraph [0096], Vallee chooses an integer r *at random* from the set of integers {0…..n}. Because the number is randomly chosen, there can be no guarantee that the number is prime, and Vallee nowhere suggests or provides for specific selection of a prime number, let alone a large prime.

Next, at paragraph [0097], Vallee computes $x = r^2 \text{mod} n$. That is, Vallee squares the randomly chosen integer (not prime, as noted above) and then finds the modulus n, where n is the last integer in the set {0….n}. This does not return a prime number, nor does it constitute multiplying two large primes, *as required in claim 5*. Again, in order to

anticipate a claim, Vallee must teach each and every element of the claim. Vallee clearly fails to teach element **(c)** because it does not find a product of first and second large primes, and therefore also cannot and does not generate or publish an encrypted value of a product of first and second large primes. Because Vallee does not teach generation or publication of encrypted values of a product of first and second large prime numbers, Vallee also cannot and does not recite decryption of such a product, as in step **(f)**.

In addition, amended claim 5 recites that a client is denied or granted access *to a secure area of a host computer* based on the prover's ability to demonstrate knowledge of a secret and product (see step **(g)**). Vallee does not recite or even suggest granting or denying access to a secure area of a host computer. Vallee only discusses providing or denying services (e.g., telecommunication equipment) or electronic funds transfer, based upon the results of an authentication attempt. See Vallee paragraphs [0176]-[0186].

The Examiner argues that Vallee's "services" are the same as a "secure area", "since the services can be information stored for access, thus secure area." Office Action page 3, item 4. Applicant respectfully disagrees. Vallee controls access to interactive services such as the Internet, cable TV, etc., but nowhere does Vallee recite storing information from those interactive services in a secure area of a host computer. To do so would be redundant, since once a client is authorized to access the interactive services they have all the necessary means to gather information directly from that interactive service. See Vallee paragraphs [0176] and [0178]. Vallee controls access to services that offer information, but does not anywhere teach providing access to information that is stored in a secure area of a host computer.

*For the sake of argument only*, even if Vallee provided information as a service (as the Examiner contends) rather than providing services that in turn offer information, Vallee still does not describe how information is obtained. Given the lack of teaching in Vallee, the Examiner appears to be making an inherency argument– namely, that entity A inherently accesses a secure area of Vallee's authenticator entity B, in order to get information. However, in order to prove inherency, the Examiner must "provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art." MPEP §2112 quoting *Ex parte Levy,* 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter.

1990), emphasis in original. The Examiner has not provided any basis in fact or technical reasoning to support the conclusion that accessing a secure area of a host (in particular, a host computer) necessarily flows from Vallee, and Applicant submits that such necessary flow cannot be shown. For example, information could be sent to entity A. Thus, the conclusion is unreasonable.

As shown above, Vallee fails to teach at least three distinct features of claim 5. Accordingly, Vallee cannot and does not anticipate the claim. Applicant respectfully requests reconsideration of claim 5, and withdrawal of the §102 rejection.

*Dependent Claim 6*: This claim depends from claim 5, and thus benefits from the above argument. Regarding the particular features of claim 6, the Examiner states that since Vallee delays authentication, and values are stored and authenticated later, Vallee anticipates claim 6. Applicant again respectfully disagrees; however, in order to clarify how previous values are used in modulus inverse operations, claim 6 is amended to recite that the previous values of the secret and product are used as operators in the modulus inverse operation, *to decrypt new values for the secret and product*. See, e.g., paragraph [0013] of the specification.

Vallee does not teach this feature; hence claim 6 is additionally allowable. Applicant thus respectfully requests withdrawal of the §102 rejection.

**Claim Rejections – 35 U.S.C. § 103 – Bartram in view of "Admission"**

Claims 1, 3, 8 and 13 stand rejected under 35 U.S.C. Section 103(a) as being unpatentable over U.S. Patent Publication No. 2004/0054885 (hereinafter, "Bartram"), in view of a purported "Admission" found at pages 1-3 of the '320 Application. Applicants respectfully traverse the rejection, for at least the following reasons.

**1. Improper use of the "Summary of the Invention" as prior art**

Applicants have pointed out that the "Summary" section "should be directed to the specific invention being claimed", MPEP 608.01(d), and that it is therefore improper to use the "Summary" section (in other words, the claimed invention), as prior art against the pending claims. The Examiner responded by stating that "The cited portion of the specification that support the statement of 'admission' are found in the background 'zero –knowledge identification protocol' (par. 3) and 'allows prover to have a set, greater than

two, of possible answers, as is provided by Fiat-Shamir protocol' (par. 10, it admits that Fiat-Shamir exists and was used as authentication)." Office Action pp./ 3-4, item 8.

Respectfully, the Examiner is mistaken. The second citation from the '320 Application, at paragraph [0010], is under the "Summary of the Invention" (which begins just prior to paragraph [0006]) and not the "Background." Accordingly, all that it "admits" is that Fiat-Shamir was used in one aspect *of Applicants' invention*. Applicants encourage the Examiner to review the '320 Application as filed. The "Summary of the Invention" section begins on page 2. Paragraph [0010] is on page 3.

**2. No evidence provided to support the assertion of obviousness**

The Examiner states that someone of ordinary skill in the art would have been able to use one protocol over the other (i.e., implementing zero-knowledge authentication) in Bartram, with reasonable expectation of success. However, the Examiner provides no basis for this opinion. Bartram itself certainly does not suggest use of zero-knowledge authentication. Indeed, as explained below, Bartram *teaches away* from zero-knowledge authentication by relying upon identification of a connecting system or certificate to determine the authentication level, and thus requires knowledge to be exchanged for authentication.

The Examiner has essentially taken a statement that zero knowledge protocol *exists*, and used that statement to justify an unsupported personal opinion as to why zero knowledge protocol could be combined with Bartram. Respectfully, this is improper. As codified in Section 2143.01 of the MPEP, *prima facie* obviousness cannot be established by merely picking and choosing unrelated features from various references. Instead, the Examiner has the additional required burden to additionally indicate in the written record where the prior art itself (absent, as in the present case, any evidence in the record of some well-known principle in the art) affirmatively teaches or suggests the motivation to combine the references as proposed. 320

Applicants have pointed out that neither the "Background" section of the '320 Application (which includes the purported "Admission") nor Bartram teach that Bartram's peer-to-peer authentication should or could be coupled with zero knowledge protocol. This remains unchallenged on the record. Applicants have also pointed out the requirement for evidence (not simply a stated opinion) to support the motivation to

combine, since neither Bartram nor the "Admission" teach or suggest any motivation to combine as proposed. However, the Examiner has not provided any such evidence and instead reiterates a personal opinion.

The Federal Circuit, though, has expressly held that mere conclusory statements from the Examiner, without any actual evidence cited on the record in support thereof, cannot satisfy the Examiner's burden to establish the obviousness of combining the references. See *In re Lee,* 277 F.3d 1338 (Fed. Cir. 2002). See also *In re KSR International Co.,* quoted above. Applicants once again submit that the Examiner must provide objective evidence that it would have been obvious, at the time the invention was made, to combine zero knowledge authentication with Bartram's peer-to-peer system; otherwise, the rejection must be withdrawn.

Without such required evidence on the record – evidence capable of objective review and rebuttal – the rejection presents nothing more than a case of impermissible hindsight. The rejection *presumes* the obviousness of combining a zero-knowledge protocol (as disclosed in Applicants' specification) with Bartram, based on the Examiner's own opinion. The Examiner, for example, has not submitted anywhere in the record how he arrived at his conclusory opinion, where he received the knowledge that forms the basis of that opinion, and the actual dates such knowledge was obtained by him. The present case therefore presents the exact situation expressly rejected by the Federal Circuit in *Lee.* The rejection of claims 1, 8 and 13 should be withdrawn for at least this reason.

**3. Bartram teaches away from use of zero knowledge authentication**

The Examiner admits that Bartram does not disclose zero-knowledge authentication/identification protocol, but states that using such protocol in Bartram would be obvious since Applicant admits that zero knowledge protocol was conventional and well known at the time the invention was made (or, alternately, because Vallee teaches using zero-knowledge). Respectfully, this cannot be correct, because Bartram teaches away from zero-knowledge authentication.

Bartram uses two (or more) levels of authentication, for example, high and low levels. Bartram suggests that the authentication method (simple acceptance; digital certificate finger print comparison; full certificate comparison, and external validation

using a certificate authority) defines the authentication level. See Bartram paragraphs [0035] and [0040]-[0044]. Note that none of these authentication methods are zero-knowledge protocols. Furthermore, note that Bartram's multiple levels of authentication rely upon the identification of the connecting system, or certificates. See, e.g., paragraphs [0031] and [0079]; see also paragraphs [0034]-[0035] for certificates and digital signatures as public and private key pairs - a concept that is very different from the zero knowledge authentication protocol wherein no certificate is exchanged.

Zero-knowledge authentication does not require any information of the connecting party in order to authenticate them. On the other hand, Bartram needs at least the identification of the connecting system, or a digital certificate (also not zero-knowledge). In addition, Bartram touts multiple levels of authentication (see, e.g., Abstract, FIG. 1). Multiple levels of authentication, as described by Bartram, are not compatible with zero-knowledge authentication. Bartram requires the transfer of information to determine the authentication level. With zero-knowledge authentication, an entity is either trusted or not trusted, and since no knowledge is exchanged during authentication, the identity of the trusted entity is not known by the authenticator. Therefore, Bartram is not compatible with zero-knowledge authentication on at least two points. Indeed, by requiring multiple levels of authentication, and by requiring identification of the connecting system/signature, Bartram *teaches away* from use of zero-knowledge protocol.

In summary, the §103 rejection of claims 1, 3 and 18 over Bartram and "Admission" fails for at least the following reasons:

1. The "Summary of the Invention" section is improperly asserted as prior art
2. The cited art itself does not support the assertion of obviousness, and no extrinsic evidence is provided to support the assertion of obviousness.
3. Bartram teaches away from use of zero knowledge authentication

Accordingly, Applicants respectfully request withdrawal of the §103 rejection of claims 1, 3, 8 and 13.

**Claim Rejections – 35 U.S.C. § 103 – Bartram in view of "Admission" and Vallee**

Claims 2, 4 and 9-12 stand rejected under 35 U.S.C. Section 103(a) as being unpatentable over Bartram and the purported Admission described above, and further in view of Vallee. Applicants again respectfully traverse the rejection.

As noted above, the purported "Admission" is partly contained in the "Summary of the Invention" section, and is therefore not an admission at all. The only remaining subject matter of the "Admission" is essentially a statement that zero-knowledge protocol *exists*; however, there is no recitation, in said "Admission" of using zero-knowledge protocol in a peer-to-peer architecture. As also noted above, Bartram teaches away from use of zero knowledge protocol in her peer-to-peer authentication, thereby countering the Examiner's opinion that zero knowledge could be incorporated into Bartram. Thus, combining with either the purported "Admission" or Vallee would be nonobvious, and, in fact, if combined with Bartram, would prevent Bartram from operating with two or more authentication levels.

Turning to the rejected claims, **claims 2 and 4** depend from claim 1. As noted above, the rejection of claim 1 is based upon an unsupported conclusory statement by the Examiner, and therefore cannot stand. Furthermore, Bartram teaches away from the combination suggested by the Examiner; thus, the rejection fails on a second count. Adding Vallee to the combination used to reject claim 1 does not solidify the rejection.

Courts have ruled that if an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071.5 USPQ2d 1596 (Fed. Cir. 1988). Since claims 2 and 4 depend from claim 1, the instant rejection fails for at least this reason.

Furthermore, **regarding claim 2**, the Examiner relies fully upon Vallee for "generating and distributing a new secret to first and second authentication agents." However, the cited passage (paragraphs [0090]-[0108]) discusses only one authenticator entity B. The other disclosed entity is an entity to be authenticated (A). There are no first and second authentication agents. Furthermore, the cited section of Vallee does not discuss generating a new secret. It is important to note that Vallee teaches the computation of secret key by a confidence authority. After the key is computed, entities A and B undergo multiple iterations of five exchange/computation steps (see steps 1-5 at Vallee paragraphs [0096]-[0100], see also paragraphs [0094] and [00101]. It appears that

the same secret key is used in each of these iterations, since there is no teaching of generating and distributing a new secret. Since claim 2 recites generation and distribution of a new secret, it contains features not taught or suggested by the Bartram/purported Admission/Vallee combination. Accordingly, *prima facie* obviousness is not established.

Applicants submitted the above arguments in support of claim 2 *verbatim* in the Response of 10 February 2009. However, the Examiner has simply repeated the rejection without a single comment to these arguments. The arguments in support of claim 2 are uncontested on the record.

Turning now to **claim 4**, the Examiner admits that Bartram and the purported Admission do not disclose the steps of claim 4. Applicants contend that, contrary to the Examiner's assertion, neither does Vallee teach these steps. For example, as noted above, Vallee does not specify *calculating a product of first and second large prime numbers*. See arguments in answer to the §102 rejections, above. Neither does Vallee generate a secret *to have a value relatively prime to the product*. For at least these reasons, the instant rejection fails. Again, Applicants submitted these exact points in the Response of 10 February 2009, but the Examiner simply repeats the rejection *verbatim*. Accordingly, the arguments in support of claim 4 remain uncontested on the record..

**Claims 9-12** depend from claim 8. As noted above, the rejection of claim 8 in view of Bartram and the purported Admission is based upon a conclusory personal opinion, and Bartram teaches away from the combination of references relied upon by the Examiner. The rejection of claim 8 therefore cannot stand. Courts have ruled that if an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071.5 USPQ2d 1596 (Fed. Cir. 1988). Thus, claims 9-12 are also nonobvious, for at least this reason. However, these claims include additional features not taught or suggested by the cited art, including the following:

In rejecting **claim 9**, the Examiner admits that Bartram and the purported Admission do not teach generating a new secret. As noted above in the arguments in support of claim 2, neither does Vallee teach this feature. Accordingly, the rejection fails

to establish *prima facie* obviousness. Once again, this argument was presented in the Response of 10 February 2009, with no response from the Examine.

**Claim 10** recites that the requesting computer comprises a cell phone. The Examiner states that the combination of Bartram and the purported Admission teach this feature, citing paragraphs 2-3 (of which reference is still not stated). Paragraph [0002] of Bartram states "With the popularity of portable computing devices (i.e., PDA's cell phones, etc.) increasing, there comes a greater need and ability to share information between devices..." The Examiner appears to argue that a zero-knowledge authentication system (including a cell phone having a prover agent) would have been obvious simply because (a) the '320 Specification recognizes that zero-knowledge protocol exists, and (b) Bartram mentions a cell phone. However, as the Examiner admits, Bartram does not teach or suggest zero knowledge authentication. Accordingly, the motivation to combine a cell phone with a zero-knowledge authentication system does not come from Bartram. In fact, as noted above, Bartram teaches away from zero-knowledge authentication.

Likewise, the '320 Background section recognizes that zero-knowledge protocol exists, but does not mention its use with a cell phone. Thus, the motivation to combine zero-knowledge authentication with a cell phone as a requesting computer also does not come from the '320 Application. And, the Examiner has not provided any evidence to support the purported combination.

Again, *prima facie* obviousness cannot be established by merely picking and choosing unrelated features from various references. Instead, the Examiner has the additional required burden to additionally indicate in the written record where the prior art itself (absent, as in the present case, any evidence in the record of some well-known principle in the art) affirmatively teaches or suggests the motivation to combine the references as proposed. See Section 2143.01 of the MPEP; see also *In re Lee*, cited above, and *Zurko,* 258 F.3d at 1385, 59 USPQ2d 1697.

Since the art itself does not teach or suggest the motivation to combine a cell phone (as a requesting computer having a prover agent) in a system of non-centralized zero-knowledge authentication, in order for the instant rejection to stand, the Examiner must provide evidence (and not a personal opinion) that such a combination would have been obvious. Otherwise, *prima facie* obviousness is not established.

Applicants have already pointed out the requirement for evidence to support the Examiner's opinion. See the Response of 10 February 2009. However, no such evidence has been provided to date. Thus, the §103 rejection of claim 10 remains insufficient (a) because there is no support for the Examiner's assertion of obviousness, and (b) because Bartram teaches away from implementing zero knowledge authentication in her peer-to-peer authentication.

**Claim 12** recites that authentication agents and prover agents are installed on each of the computers through common software. The Examiner appears to rely upon Bartram paragraphs 25-34 for this feature; however, this passage does not discuss authentication or prover agents. It discusses collaborative application software (i.e., software 104, FIG. 1), but authentication and prover agents are not mentioned.

Furthermore, this section of Bartram discusses the exchange of certificates between computers. This is different from engaging in zero-knowledge protocol, as in base claim 8. As noted with respect to claims 1, 8 and 13, above, the acknowledgement that zero-knowledge protocol exists (in the '320 Application "Background" section) does not itself establish obviousness of a system where a requesting computer operates with an authentication agent on the network, once it is itself authenticated to the network via zero-knowledge protocol. The cited art itself does not teach or suggest the motivation to make the proposed combination, and the Examiner has not provided any documentary evidence for why such a combination would have been obvious. Furthermore, Bartram teaches away from use of zero knowledge protocol in peer-to-peer authentication. Accordingly, the instant rejection is deficient and should be withdrawn.

Once more, the above arguments were presented to the Examiner in Applicants' Response of 10 February 2009; however, the Examiner has not addressed the arguments, instead repeating the rejection *verbatim*. Applicant respectfully requests that the Examiner carefully review all of the above arguments. Applicant believes that all rejections presented in the May 20, 2009 Office Action are overcome by the above amendments and remarks. However, if any rejection is repeated, Applicants respectfully request that the Examiner respond to the substance of Applicants' arguments and provide evidence to support a conclusion of obviousness.

## CONCLUSION

It is believed that the above remarks address and overcome each rejection presented in the office action of 20 May 2009. Applicants thus respectfully solicit a Notice of Allowance for all pending claims. Should any of the instant rejections be reiterated, Applicants again respectfully request that the Examiner respond specifically to Applicants arguments, and provide evidence to support a conclusion of obviousness, where the references themselves do not suggest the relied-upon combinations.

Per MPEP §706.07, "The examiner should never lose sight of the fact that in every case the applicant is entitled to a full and fair hearing, and that a clear issue between applicant and examiner should be developed, if possible, before appeal." Failing to respond to Applicants' arguments (and instead repeating prior rejections *verbatim*) does not allow for the development of clear issues.

A Petition for One Month's Extension of Time is filed herewith, along with authorization to charge the required petition fee to Deposit Account No. 12-0600. This extends the period of reply up to, and including, 20 September 2009. Given that 20 September 2009 fell upon a Sunday, this paper is timely filed today, Monday, 21 September 2009.

No fees are due for new claims 14 or 15, since the '320 Application now includes 3 independent claims and 15 dependent claims (within the number of independent and dependent claims allowed without additional claim fees). No other fees are believed due; however, if any additional fee is deemed necessary in connection with this paper, please charge the aforementioned Deposit Account. Should any issues remain outstanding, the Examiner is encouraged to telephone the undersigned.

Respectfully submitted,
LATHROP & GAGE LLP

Date: 21 Sept. 2009

By: Heather Perrin

Heather Perrin, Reg. No. 52,884
4845 Pearl East Circle, Suite 201
Boulder, Colorado 80301
Tel No: (720) 931-3033
Fax No: (720) 931-3001